IN THE CLAIMS:

1-15. (Cancelled)

16. (Original) A file encryption apparatus that encrypts a plaintext to generate a ciphertext and stores the ciphertext into a memory unit thereof, the file management apparatus comprising:

a key storage medium storing key information beforehand;

registration means for receiving an input of a password, encrypts the key information using the received password to generate an encrypted key, and writes the generated encrypted key to the memory unit; and

encryption unit means for encrypting a plaintext using a file key to generate a ciphertext, encrypting the file key using the key information to generate an encrypted file key, and writing the ciphertext in association with the encrypted file key, to the memory unit.

17. (Original) A file decryption apparatus that stores the ciphertext and the encrypted file key generated by the file encryption apparatus of Claim 16, in association with each other, in a memory unit thereof, and decrypts the ciphertext, the file decryption apparatus comprising:

a key storage medium storing key information beforehand;

switch means

(a) including first key obtaining means for receiving an input of a password and decrypting the encrypted key using the received password to generate key information, and second key obtaining means for reading the key information from the key storage medium, and

(b) obtaining the key information by one of the first key obtaining means and the second key obtaining means; and

decryption means for decrypting the encrypted file key using the obtained key information to generate a file key, and decrypts the ciphertext using the file key to generate a decrypted text.

18-37. (Cancelled)

Please add the newly drafted Claims 38-43.

38. (New) A file encryption apparatus that encrypts a plaintext to generate a ciphertext and stores the ciphertext into a memory unit thereof, the file management apparatus comprising:

a key storage medium storing key information beforehand;

registration unit for receiving an input of a password, encrypts the key information using the received password to generate an encrypted key, and writes the generated encrypted key to the memory unit; and

encryption unit for encrypting a plaintext using a file key to generate a ciphertext, encrypting the file key using the key information to generate an encrypted file key, and writing the ciphertext in association with the encrypted file key, to the memory unit.

39. (New) A file decryption apparatus that stores the ciphertext and the encrypted file key generated by the file encryption apparatus of Claim 38, in association with each other, in a memory unit thereof, and decrypts the ciphertext, the file decryption apparatus comprising:

a key storage medium storing key information beforehand;

switch unit

(a) including a first key obtaining unit for receiving an input of a password and decrypting the encrypted key using the received password to generate key information, and a second key obtaining unit for reading the key information from the key storage medium, and

(b) obtaining the key information by one of the first key obtaining unit and the second key obtaining unit; and

a decryption unit for decrypting the encrypted file key using the obtained key information to generate a file key, and decrypts the ciphertext using the file key to generate a decrypted text.

40. (New) The file decryption apparatus of Claim 39,

wherein the registration unit further receives an input of a user identifier that identifies a user, and writes the user identifier in association with the encrypted key, to the memory unit, and

the first key obtaining unit further receives an input of the user identifier and decrypts the encrypted key that is associated with the user identifier.

41. (New) The file decryption apparatus of Claim 39,

wherein the registration unit further writes the key information and/or authentication information in association with the encrypted key, to the memory unit,

the encryption unit further writes the encrypted key, the key information, and/or authentication information in association with the ciphertext, to the memory unit,

the first key obtaining means checks, using the authentication information, whether the encrypted key has been altered or not, when the encrypted key that is associated with the authentication information is decrypted, and

the decryption unit checks, using the authentication information, whether the ciphertext has been altered or not, when the ciphertext that is associated with the authentication information is decrypted.

42. (New) The file decryption apparatus of Claim 34,

wherein the registration unit writes the encrypted key to the memory unit that is a portable storage medium, and

the first key obtaining unit decrypts the encrypted key that has been written to the memory unit that is the portable storage medium.

43. (New) The file management apparatus of Claim 38, further comprising

a deletion unit for deleting the encrypted key that has been written to the memory unit,

wherein the registration unit further receives an input of a new password, encrypts the key information using the new password to generate a new encrypted key, and writes the generated new encrypted key to the memory unit.